EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 11143780
PUBLICATION DATE : 28-05-99

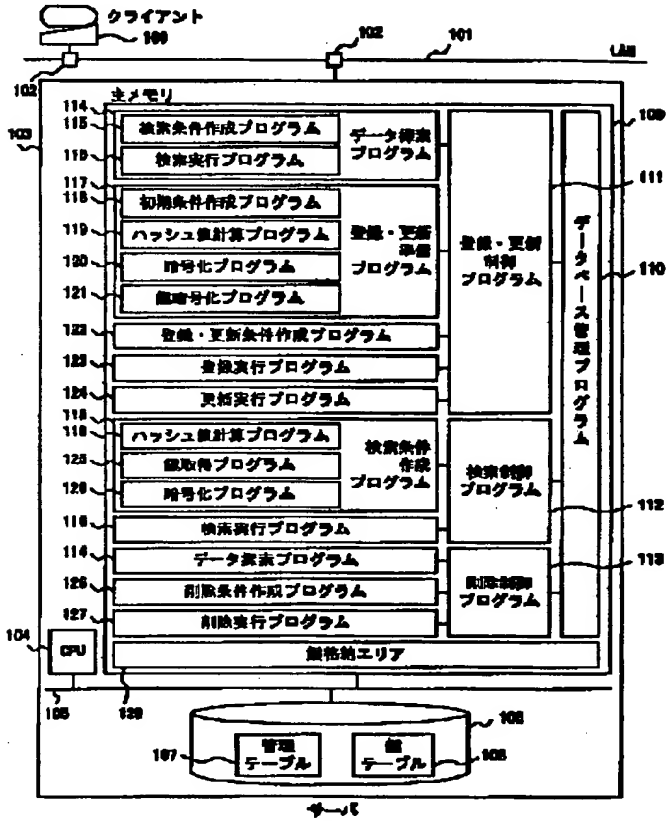
APPLICATION DATE : 05-11-97
APPLICATION NUMBER : 09319010

APPLICANT : HITACHI LTD;

INVENTOR : MATSUNAGA KAZUO;

INT.CL. : G06F 12/14 G06F 12/00 G06F 17/30 G09C 1/00 G09C 1/00

TITLE : METHOD AND DEVICE FOR MANAGING SECRET INFORMATION IN DATABASE



ABSTRACT : PROBLEM TO BE SOLVED: To improve the flexibility and stability of and database to be enciphered by managing information related with encipherment through the use of an exclusive table.

SOLUTION: Encipherment data are managed by a management table 107 of a database to be enciphered and a key table 108 corresponding to the table. The key table 108 has a cryptographic key, an encipherment algorithm identifier, and a data hash value for each group of specific values (the item, line, and column of one column in one line). At each time of the registration or update of data for the management table 107, the cryptographic key is generated by a data encipherment program 112, and the cryptographic key is enciphered by using a key cryptographic key, and registered in the key table 108. Retrieval of the enciphered data is operated by deciphering the cryptographic key obtained by the hash value by using the key cryptographic key, and using the deciphered cryptographic key and the encipherment algorithm. Thus, change of the cryptographic key or the encipherment algorithm can be attained during database activation.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－143780

(43)公開日　平成11年(1999)５月28日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ
	12/00	５３７		12/00	５３７Ｈ
	17/30		Ｇ０９Ｃ	1/00	６３０Ａ
Ｇ０９Ｃ	1/00	６３０			６６０Ｄ
		６６０	Ｇ０６Ｆ	15/40	３２０Ａ

審査請求　未請求　請求項の数10　ＦＤ　（全 22 頁）

(21)出願番号　特願平9－319010

(22)出願日　平成９年(1997)11月５日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　茶谷　謙一
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報・通信開発本部内

(72)発明者　北川　誠
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報・通信開発本部内

(72)発明者　松永　和男
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

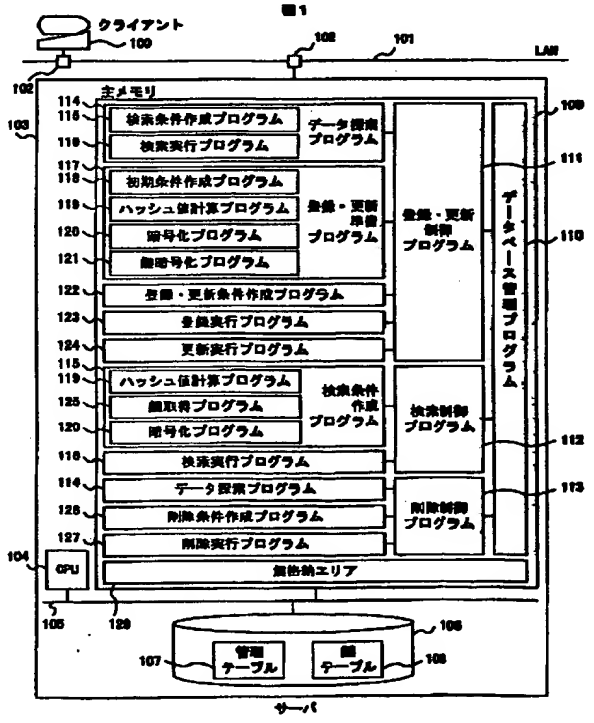
(74)代理人　弁理士　笹岡　茂　（外１名）

(54)【発明の名称】　データベースにおける秘密情報管理方法およびデータベースの秘密情報管理装置

(57)【要約】

【課題】　暗号化に関する情報を専用のテーブルを使って管理することにより、暗号化するデータベースの柔軟性と安全性を向上する。

【解決手段】　暗号化するデータベースの管理テーブル１０７とそのテーブルに対応する鍵テーブル１０８により、暗号化データを管理する。鍵テーブル１０８は特定の値の集合（１つの行の中の１つの列の項目、行、列）ごとに暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値を持つ。管理テーブル１０７へのデータの登録または更新ごとにデータ暗号化プログラム１１２において暗号鍵を作成し、さらに該暗号鍵を鍵暗号鍵を用いて暗号化し、これを鍵テーブル１０８に登録する。暗号データの検索は、ハッシュ値によって得られる暗号鍵を鍵暗号鍵を用いて復号し、復号した暗号鍵と暗号化アルゴリズムを用いて行う。これによりデータベース稼動中に暗号鍵や暗号化アルゴリズムの変更を可能にする。



【特許請求の範囲】

【請求項１】　暗号化された秘密情報を管理するデータベースにおける秘密情報管理方法であって、
前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを設け、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、
前記データベースへの秘密情報の登録時に、
シリアル番号を作成し、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録し、
前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化し、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算し、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録することを特徴とするデータベースにおける秘密情報管理方法。

【請求項２】　請求項１記載の秘密情報管理方法において、
前記データベースに登録された秘密情報の検索時に、
検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出し、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出し、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号し、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行うことを特徴とするデータベースにおける秘密情報管理方法。

【請求項３】　請求項２記載のデータベースにおける秘密情報管理方法において、
検索条件に一致する秘密情報を検索後に、
該検索した秘密情報を暗号化するための新たな鍵を乱数を使って作成し、該作成した鍵により該検索した秘密情報を暗号アルゴリズムを用いて新たに暗号化し、該作成した鍵を前記鍵暗号鍵により暗号化し、該新たに暗号化した秘密情報で管理テーブルを更新し、前記鍵暗号鍵により暗号化した暗号化のための新たな鍵と前記暗号アルゴリズムの識別子により鍵テーブルを更新することを特徴とするデータベースにおける秘密情報管理方法。

【請求項４】　請求項２記載のデータベースにおける秘密情報管理方法において、
前記データベースに登録された秘密情報の更新時に、
更新前の秘密情報と更新後の秘密情報を入力し、更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得し、
前記更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録し、
前記作成した鍵を前記鍵暗号鍵により暗号化し、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録することを特徴とするデータベースにおける秘密情報管理方法。

【請求項５】　暗号化された秘密情報を管理するデータベースの秘密情報管理装置であって、
前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、
秘密情報の登録時にシリアル番号を作成する手段と、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化する手段と、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録する手段と、
前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手段と、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算する手段と、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録する手段と、
秘密情報の検索時に検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出す手段と、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出す手段と、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号する

手段と、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行う手段を備えることを特徴とするデータベースの秘密情報管理装置。

【請求項６】　請求項５記載のデータベースの秘密情報管理装置において、

秘密情報の更新時に、入力された更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得する手段と、入力された更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化する手段と、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録する手段と、

前記作成した鍵を前記鍵暗号鍵により暗号化する手段と、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録する手段を備えることを特徴とするデータベースにおけるデータベースの秘密情報管理装置。

【請求項７】　暗号化された秘密情報と暗号化に用いた鍵情報を記録したコンピュータ読み取り可能な記録媒体であって、

前記暗号化された秘密情報は管理テーブルに記録され、

前記暗号化に用いた鍵情報は鍵テーブルに記録され、

前記管理テーブルは、複数の行と複数の列からなり、各行対応に暗号化された秘密情報の組が記録され、

前記鍵テーブルは、複数の行と複数の列からなり、前記管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値が記録され、

前記管理テーブルと鍵テーブルの各行には管理テーブルの行と鍵テーブルの行を互いに関連付けるシリアル番号が記録されたことを特徴とする暗号化された秘密情報と暗号化に用いた鍵情報を記録したコンピュータ読み取り可能な記録媒体。

【請求項８】　暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースへの秘密情報の登録時にシリアル番号を作成する手順と、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化する手順と、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録する手順と、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手順と、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算する手順と、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録する手順を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項９】　暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースへの秘密情報の検索時に検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出す手順と、該条件一致行から、秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出す手順と、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号する手順と、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行う手順を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを備え、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けしたデータベースを管理する秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記データベースに登録された秘密情報の更新時に、入力された更新前の秘密情報によりデータベースを検索

し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得する手順と、入力された更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化する手順と、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録する手順と、前記作成した鍵を秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化する手順と、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録する手順を実行させる秘密情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、秘密情報をデータベースに暗号化して登録し、管理する方法に関するものである。

【０００２】

【従来の技術】昨今、データベースは、クレジット会社、銀行など様々な分野で利用されている。特に最近では、電子商取引の認証を行う認証局も、認証のために氏名やクレジット番号などの個人の秘密情報を管理するデータベースを持っている。このようなデータベースは個人に関する秘密情報を扱っているため、例えばデータベースを操作できるアクセス権をデータベース管理者のような特定の個人にしか与えないようにすることにより、データの漏洩を防いでいる。しかしながら、データベースへのアクセス権を設定している場合でも、不正な侵入者がデータベースを記録した記憶装置を不正に持ち出し、該装置の内容を直接見ることによりデータが漏洩する危険性がある。そこで、氏名やクレジット番号など特定の情報を暗号化して登録し、情報を取り出すときに復号して元の情報を得ることによりセキュリティを確保することが考えられる。このように特定の情報を暗号化しておくことにより、データベースが記録された装置が盗難にあったとしても復号のための鍵が盗まれていなければ、情報が漏洩する危険性は大幅に減少する。従来は、このような情報の暗号化に特定の一つの鍵を用いて、データベース全体を暗号化していた。

【０００３】データベースを暗号化する技術の例としては「特開平８－３２９０１１」に開示されているものがある。該公知例の実施例は、データベース、鍵管理センタ、１次ユーザ、２次ユーザを相互に接続するネットワークシステムから構成される。１次ユーザは著作権情報を暗号化してデータベースに格納し、鍵を鍵管理センタに格納する。２次ユーザがその著作権情報を利用するときは、鍵管理センタから暗号鍵をもらい、そのときに課金される方式が提案されている。この公知例の鍵管理センタは、保管されている鍵と著作権ラベルの対応づけを行うことによって鍵を管理している。

【０００４】

【発明が解決しようとする課題】従来の技術では、特定の一つの暗号鍵でデータベース全体を暗号化したデータベースでは、その暗号鍵がデータベースが記録された装置と同時に盗難にあった場合、データベース全体が解読され、秘密情報が漏洩する危険性がある。また、データベースの稼動中に暗号鍵が盗難にあった場合、不正侵入者がこの鍵を使用してデータを解読する可能性がある。従って、これらの状況においては暗号鍵を変更してデータの漏洩を防止する必要が生じる。暗号鍵を変更するためには、データベースに対するユーザからのアクセスを禁止し、データベース中のすべてのデータを一旦復号化した後で新しい暗号鍵で暗号化し直さなければならない。データベースの規模が大きくなればなるほどこの作業には時間がかかり、その間、ユーザはデータベースにアクセスできない。さらに鍵が盗難に会わなくとも、暗号化されたデータのうち一つが解読されると、データベースを暗号化している鍵が一つであるため、他のデータがすべて解読される危険性がある。

【０００５】また、従来の技術ではデータベースの稼動中に、より強固な暗号化アルゴリズムを採用してセキュリティを高めようとする場合に、暗号化アルゴリズムを変更することが困難である。なぜなら、この場合にもデータベースへのユーザアクセスを一旦禁止し、すべてのデータを新しい暗号化アルゴリズムで暗号化し直さなければならないからである。以上で述べたように、従来のデータベースを暗号化する方式においては、データベースを暗号化する鍵が１つであるためその鍵が盗難に合った場合、その鍵で暗号化されたデータベースがすべて解読され秘密情報が漏洩する危険性があり、また暗号化したデータベース稼働中により強固な暗号化アルゴリズムが発明されたとしてもデータベースの暗号化アルゴリズムをその方式に変更するのは困難であるという問題があった。

【０００６】本発明は、データベースを暗号化する方式において、データベースの内容を漏洩しない安全なデータベースの秘密情報管理方式を提供すること、暗号鍵や暗号化アルゴリズムの変更をデータベース稼働中にも容易に行うことができるようにすること、および複数の暗号化アルゴリズムと複数の暗号鍵を使うことができるようにすることを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号化された秘密情報を管理するデータベースにおける秘密情報管理方法であって、前記データベースに、暗号化された秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム

識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルを設け、該管理テーブルと鍵テーブルに行ごとにシリアル番号を付与して互いに関連付けし、前記データベースへの秘密情報の登録時に、シリアル番号を作成し、登録する秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により前記管理テーブルに登録する秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した秘密情報を前記シリアル番号と共に前記管理テーブルに登録し、前記作成した鍵を、該作成した鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する鍵暗号鍵により暗号化し、暗号化された秘密情報の検索のために使用する前記ハッシュ値を計算し、該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と、前記暗号アルゴリズムの識別子と、前記検索のためのハッシュ値を前記シリアル番号と共に前記鍵テーブルに登録するようにしている。

【０００８】また、前記データベースに登録された秘密情報の検索時に、検索条件のハッシュ値を求め、前記鍵テーブルから該検索条件のハッシュ値に一致するハッシュ値を有する条件一致行を取り出し、該条件一致行から前記鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵と暗号アルゴリズム識別子の組を取り出し、取り出した該鍵暗号鍵により暗号化された秘密情報の暗号化のための鍵を該鍵暗号鍵により復号し、該復号した鍵と前記暗号アルゴリズム識別子に対応する暗号アルゴリズムにより前記検索条件を暗号化し、該暗号化された検索条件により前記管理テーブルの検索を行うようにしている。

【０００９】また、検索条件に一致する秘密情報を検索後に、該検索した秘密情報を暗号化するための新たな鍵を乱数を使って作成し、該作成した鍵により該検索した秘密情報を暗号アルゴリズムを用いて新たに暗号化し、該作成した鍵を前記鍵暗号鍵により暗号化し、該新たに暗号化した秘密情報で管理テーブルを更新し、前記鍵暗号鍵により暗号化した暗号化のための新たな鍵と前記暗号アルゴリズムの識別子により鍵テーブルを更新するようにしている。

【００１０】また、前記データベースに登録された秘密情報の更新時に、更新前の秘密情報と更新後の秘密情報を入力し、更新前の秘密情報によりデータベースを検索し、該更新前の秘密情報の存在する前記管理テーブルのシリアル番号を取得し、前記更新後の秘密情報を暗号化するための鍵を乱数を使って作成し、該作成した鍵により該更新後の秘密情報を暗号アルゴリズムを用いて暗号化し、該暗号化した更新後の秘密情報を前記管理テーブルの前記取得したシリアル番号の行に登録し、前記作成した鍵を前記鍵暗号鍵により暗号化し、該鍵暗号鍵により暗号化した鍵と、前記暗号アルゴリズムの識別子を前記鍵テーブルの前記取得したシリアル番号の行に登録するようにしている。

【００１１】

【発明の実施の形態】まず、本発明の原理について説明する。秘密情報を管理するデータベースは、暗号化された秘密情報を格納するための管理テーブルと、その管理テーブルの１つの行の中の１つの列の項目（以下では、フィールドと称する）、行、または列などの特定の値の集合ごとに該集合に属する個々の値を暗号化するために使用した鍵と暗号アルゴリズム識別子を格納する鍵テーブルを有する。前記管理テーブルと鍵テーブルは、２つのテーブルの行を関連付けるシリアル番号をそれぞれ格納しており、前記管理テーブルの特定の値の集合を結合した値に対して計算したハッシュ値も鍵テーブルに格納する。暗号化した秘密情報の登録には、まず、秘密情報を暗号化するための鍵（以下では、データ暗号鍵と称する）を乱数を使って作成する。そのデータ暗号鍵を使って管理テーブルに登録する秘密情報を暗号化する。このような鍵の例としてＭＵＬＴＩ２、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）等がある。さらに、前記データ暗号鍵は、秘密情報を暗号化する鍵とは別に作成した鍵であって管理テーブルに登録する秘密情報を暗号化したすべての鍵の暗号化に使用する別の鍵（以下では、鍵暗号鍵と称する）を用いて暗号化される。そして、秘密情報の検索のために使用するハッシュ値を暗号化前の秘密情報から計算する。さらに、シリアル番号を生成し、シリアル番号と暗号化された秘密情報を管理テーブルに登録し、シリアル番号とデータ暗号鍵と暗号化アルゴリズム識別子とハッシュ値を鍵テーブルに登録する。

【００１２】検索条件としてシリアル番号が指定された場合は、鍵テーブルにおいてそのシリアル番号を検索し、鍵テーブルからそのシリアル番号に一致する暗号化アルゴリズム識別子と暗号化されたデータ暗号鍵を取り出し、鍵暗号鍵で暗号化されたデータ暗号鍵を復号する。次に管理テーブルにおいてシリアル番号を検索し、管理テーブルから、シリアル番号に一致する暗号化された秘密情報を取り出し、その秘密情報を前記暗号アルゴリズムで前記データ暗号鍵を使って復号する。検索条件として秘密情報のみが指定された場合は、まず、検索条件のハッシュ値を計算する。そのハッシュ値により鍵テーブルを検索してそのハッシュ値に一致する暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子をすべて取り出し、前記暗号化されたデータ暗号鍵を復号したデータ暗号鍵と、暗号化アルゴリズムにより検索条件を暗号化する。次に、暗号化した検索条件を使って管理テーブルを検索し、一致する秘密情報を含む行が見つかった場合、その行のシリアル番号に対応する鍵テーブルの他の暗号化されたデータ暗号鍵を復号した鍵と暗号化アルゴリズム識別子を使って、検索条件以外の秘密情報を復号する。

【００１３】以上説明した原理を、さらに具体例を用いて説明する。本例で用いる管理テーブルの例を図２に示し、その管理テーブルに対応する鍵テーブルを図３に示す。管理テーブルの列は、シリアル番号、名前、電話番号、住所で構成され、鍵テーブルの列は、シリアル番号、名前のハッシュ値、名前暗号アルゴリズム識別子、名前の暗号鍵、電話番号のハッシュ値、電話番号暗号アルゴリズム識別子、電話番号の暗号鍵、住所のハッシュ値、住所暗号アルゴリズム識別子、住所の暗号鍵で構成される。図２、図３において、天地逆の文字は暗号化されているデータを示している。図２の管理テーブルには、名前、電話番号が暗号化され、住所が暗号化されないで格納されている。図３の鍵テーブルには、名前、電話番号、住所のそれぞれのハッシュ値、暗号化アルゴリズム識別子、暗号鍵が格納され、このうち暗号鍵は暗号化されて格納されている。

【００１４】本例で、シリアル番号の項目２００の列が「１１」の行２０４と、シリアル番号の項目２００の列が「１２」の行２０５が、管理テーブルに格納されており、シリアル番号の項目３００の列が「１１」の行３１０と、シリアル番号の項目３００の列が「１２」の行３１１が、鍵テーブル１０８に格納されている状態で、新たに名前「日立花子」、電話番号「９８７－６５４３」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「９８７－６５４３」を暗号化するための鍵を乱数を使ってそれぞれ作成し、「３１５ＴＫ８」「１２３ＡＢＤ」を求める。次に作成した鍵「３１５ＴＫ８」を使って「日立花子」を暗号化プログラムが持つ最新の暗号アルゴリズムで暗号化し、鍵「１２３ＡＢＤ」を使って「９８７－６５４３」を前記暗号アルゴリズムで暗号化する。次に「日立花子」からハッシュ値「５０２」を計算し、「９８７－６５４３」からハッシュ値「１４３」を計算し、「東京都」からハッシュ値「１２３」を計算する。鍵「３１５ＴＫ８」、「１２３ＡＢＤ」を鍵暗号鍵で暗号化する。管理テーブルと鍵テーブルの行を関係付けるシリアル番号「１３」を生成し、管理テーブルのシリアル番号の項目２０７に「１３」、名前の項目２０８に暗号化された「日立花子」、電話番号の項目２０９に暗号化された「９８７－６５４３」、住所の項目２１０に「東京都」を登録し、鍵テーブルのシリアル番号の項目３１２に「１３」、名前のハッシュ値の項目３１３に「５０２」、名前の暗号化アルゴリズム識別子の項目３１４に「２」、名前の暗号鍵の項目３１５に暗号化された「３１５ＴＫ８」、電話番号のハッシュ値の項目３１６に「１４３」、電話番号の暗号化アルゴリズム識別子の項目３１７に「２」、電話番号の暗号鍵の項目３１８に暗号化された「１２３ＡＢＤ」、住所のハッシュ値の項目３１９に「１２３」、住所の暗号化アルゴリズム識別子の項目３２０に「０」を登録する。

【００１５】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」の電話番号を検索する場合について説明する。まず、「日立二郎」からハッシュ値を計算し、ハッシュ値「３５９」を求める。鍵テーブルの名前のハッシュ値で「３５９」を検索して、その暗号化アルゴリズム識別子「１」３２２と暗号化されたデータ暗号鍵「ＺＸＢ５１５」３２３を取り出す。次にデータ暗号鍵を鍵暗号鍵で復号する。復号した暗号鍵「ＺＸＢ５１５」３２３と暗号化アルゴリズム識別子「１」３２２を使って名前の検索条件「日立二郎」を暗号化する。暗号化された「日立二郎」の検索条件を使って管理テーブルを検索する。管理テーブルにおいて暗号化された「日立二郎」を検索し、その行のシリアル番号「１２」２１１を取り出し、そのシリアル番号「１２」２１１を使って鍵テーブルの電話番号の暗号化アルゴリズム識別子「１」３２４と暗号化されたデータ暗号鍵「０１ＥＲ８８」を鍵暗号鍵で復号した鍵を使って管理テーブル上の「日立二郎」の暗号化された電話番号を復号化する。

【００１６】次に、各行に含まれる値のそれぞれに同一のデータ暗号鍵を使用し、かつ各行ごとに異なるデータ暗号鍵を使用する場合について説明する。この場合の管理テーブルと鍵テーブルの例を図４、図５に示す。図４は、行ごとに暗号化された管理テーブルの例である。図４のテーブル構成は図２と同じであるが、暗号化されて格納されている単位が図２と異なり、行ごとになっている。図４において、天地逆の文字は暗号化されているデータを示している。図４の管理テーブルに対応する鍵テーブルの例を図５に示す。図５の鍵テーブルは、シリアル番号、名前と電話番号を連結した値のハッシュ値、暗号化アルゴリズム識別子、およびデータ暗号鍵を列に持つ。鍵テーブルは行ごとに暗号化した鍵を持つのでハッシュ値、暗号化アルゴリズム識別子、暗号鍵は行ごとに１つだけ存在する。図５において、天地逆の文字は暗号化されているデータを示している。シリアル番号の項目の列５００は、管理テーブルと鍵テーブルの行を関連付けるためのシリアル番号を格納する。図５では、名前、電話番号の２つを組み合わせて計算されるハッシュ値を、名前、電話番号のハッシュ値の項目の列５０１に格納しているが、これは名前だけの１つからハッシュ値を計算するようにしてもよい。図４の管理テーブルと図５の鍵テーブルの構造を持つデータベースにより、行ごとにそれぞれ別のデータ暗号鍵で暗号化することが可能となる。

【００１７】本例で、シリアル番号の項目の列４００が「１１」の行４０４と、シリアル番号の項目の列４００が「１２」の行４０５が、管理テーブルに格納されており、シリアル番号の項目の列５００が「１１」の行５０４と、シリアル番号の項目の列５００が「１２」の行５０５が、鍵テーブルに格納されている状態で、新たに名

前「日立花子」、電話番号「９８７－６５４３」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「９８７－６５４３」、「東京都」を暗号化するための鍵を乱数を使って１つ作成し、「３１５ＴＫ８」を求める。次に作成した鍵「３１５ＴＫ８」を使って「日立花子」、「９８７－６５４３」、「東京都」をそれぞれ暗号化プログラムが持つ最新の暗号アルゴリズムで暗号化する。次に「日立花子」、「９８７－６５４３」からハッシュ値「５３２」を計算する。鍵「３１５ＴＫ８」を鍵暗号鍵で暗号化する。管理テーブルと鍵テーブルの行を関係付けるシリアル番号「１３」を生成し、管理テーブルのシリアル番号の項目４０７に「１３」、名前の項目４０８に暗号化された「日立花子」、電話番号の項目４０９に暗号化された「９８７－６５４３」、住所の項目４１０に暗号化された「東京都」を登録し、鍵テーブルのシリアル番号の項目５０６に「１３」、名前、電話番号のハッシュ値の項目５０７に「５３２」、暗号化アルゴリズム識別子の項目５０８に「１」、暗号鍵の項目５０９に暗号化された「３１５ＴＫ８」を登録する。

【００１８】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」で電話番号が「１２３－４５６７」の住所を検索する場合について説明する。行ごとに暗号化されたデータベースにおいて暗号化された情報を検索する場合、ハッシュ値を計算するために使用した項目はすべて検索条件の中に指定しなければならない。まず、「日立二郎」、「１２３－４５６７」からハッシュを計算し、ハッシュ値「４５９」を求める。鍵テーブルの名前、電話番号のハッシュ値で「４５９」を検索して、その暗号化アルゴリズム識別子「１」５１２と暗号化されたデータ暗号鍵「ＰＢ２４ＣＳ」５１３を取り出す。次にデータ暗号鍵を鍵暗号鍵で復号する。

【００１９】取り出した暗号鍵「ＰＢ２４ＣＳ」５１３と暗号化アルゴリズム識別子「１」５１２を使って「日立二郎」、「１２３－４５６７」を暗号化した検索条件を作成する。暗号化された「日立二郎」、「１２３－４５６７」の検索条件を使って管理テーブルを検索する。管理テーブルにおいて暗号化された「日立二郎」、「１２３－４５６７」を検索し、一致する行が管理テーブルにあれば、「日立二郎」、「１２３－４５６７」を暗号化した鍵と暗号化アルゴリズムを使って、シリアル番号が「１２」の行の管理テーブルの暗号化された住所を復号化する。

【００２０】暗号化する特定の集合が列の場合の管理テーブルと鍵テーブルの例を図６、図７に示す。図６のテーブル構成はシリアル番号の項目がない点が図２と異なる。図６において、天地逆の文字は暗号化されているデータを示している。図６では住所の項目６０２のデータは暗号化されないで格納されている。図６の管理テーブルに対応する鍵テーブルの例を図７に示す。図７において、天地逆の文字は暗号化されているデータを示している。図７は、各列に含まれる値のそれぞれに同一のデータ暗号鍵を使用し、かつ各列ごとに異なるデータ暗号鍵を使用する場合の鍵テーブルの例である。この場合は、列ごとにすべての行が同じ暗号鍵と暗号化アルゴリズムを使うので、ハッシュ値を格納しない。図６の管理テーブルと図７の鍵テーブルの構造を持つデータベースにより、列ごとにそれぞれ別の暗号鍵を持つデータベースの暗号化が可能となる。

【００２１】本例で、管理テーブルの行６０３と行６０４が、管理テーブルに格納されており、行７１１が、鍵テーブルに格納されている状態で、新たに名前「日立花子」、電話番号「９８７－６５４３」、住所「東京都」をデータベースに登録する場合の手順について説明する。まず、「日立花子」、「９８７－６５４３」を暗号化するための鍵を取得する。そのために鍵暗号鍵で暗号化された「２４Ｂ５２Ｃ」、「ＳＷ６１０Ｖ」と暗号アルゴリズム識別子「１」、「１」を鍵テーブルから取得し、鍵暗号鍵で暗号化された「２４Ｂ５２Ｃ」、「ＳＷ６１０Ｖ」を鍵暗号鍵で復号する。次に取得した鍵「２４Ｂ５２Ｃ」を使って「日立花子」を鍵テーブルから取り出した暗号アルゴリズムで暗号化し、鍵「ＳＷ６１０Ｖ」を使って「９８７－６５４３」を前記暗号化アルゴリズムで暗号化する。

【００２２】次に、この秘密情報データベース（管理テーブルと鍵テーブル）から、名前が「日立二郎」の電話番号を検索する場合について説明する。まず、鍵テーブルから名前の暗号化アルゴリズム識別子「１」７０６と暗号化されたデータ暗号鍵「２４Ｂ５２Ｃ」７０７を取り出す。次に暗号化されたデータ暗号鍵「２４Ｂ５２Ｃ」を鍵暗号鍵で復号する。前記データ暗号鍵「２４Ｂ５２Ｃ」７０７を暗号化アルゴリズム識別子「１」７０６を使って名前の検索条件「日立二郎」を暗号化する。暗号化された「日立二郎」の検索条件を使って管理テーブルを検索する。「日立二郎」の行の暗号化された電話番号を鍵テーブルの電話番号の暗号鍵「ＳＷ６１０Ｖ」７０９を復号化したものと暗号化アルゴリズム識別子「１」を使って復号化する。

【００２３】以上のように、秘密情報を暗号化して登録するデータベースにおいて、暗号化した秘密情報を格納する管理テーブルと、該管理テーブルの特定の値の集合（１つの行の中の１つの列の項目、行、列など）対応に該集合に属する各値を暗号化するために使用した鍵と暗号アルゴリズム識別子と該管理テーブルの特定の値の集合対応に求められた該集合のハッシュ値を格納する鍵テーブルの２つを使って管理することにより、管理テーブルの特定の値の集合ごとに暗号鍵と暗号化アルゴリズムを変更することが可能となる。

【００２４】以下、本発明の第一の実施例について図１

を用いて説明する。本システムは、クライアント１００、ＬＡＮ１０１、ＬＡＮアダプタ１０２、サーバ１０３から構成される。クライアント１００とサーバ１０３は、ＬＡＮアダプタ１０２を介してＬＡＮ１０１により接続される。サーバ１０３は、ＣＰＵ１０４、主メモリ１０９、バス１０５、磁気ディスク装置１０６から構成される。主メモリ１０９と磁気ディスク装置１０６は、ＣＰＵ１０４よりバス１０５を介してアクセスされる。主メモリ１０９には、データベース管理プログラム１１０、登録・更新制御プログラム１１１、検索制御プログラム１１２、削除制御プログラム１１３、データ探索プログラム１１４、登録・更新準備プログラム１１７、登録・更新条件作成プログラム１２２、登録実行プログラム１２３、更新実行プログラム１２４、検索条件作成プログラム１１５、検索実行プログラム１１６、削除条件作成プログラム１２６、削除実行プログラム１２７および鍵格納エリア１２８が格納される。

【００２５】データ探索プログラム１１４は、検索条件作成プログラム１１５と検索実行プログラム１１６で構成される。登録・更新準備プログラム１１７は、初期条件作成プログラム１１８、ハッシュ値計算プログラム１１９、暗号化プログラム１２０、および鍵暗号化プログラム１２１で構成される。検索条件作成プログラムは、ハッシュ値計算プログラム１１９、鍵取得プログラム１２５、および暗号化プログラム１２０で構成される。磁気ディスク装置１０６には、管理テーブル１０７と鍵テーブル１０８が格納される。

【００２６】以下、図１の構成のシステムにおいて、データベースに暗号化して格納するデータの登録処理の概略について説明する。ユーザがクライアント１００からデータベースに登録するデータを入力する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力された登録するデータが登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、登録・更新準備プログラム１１７に登録するデータを渡す。登録・更新準備プログラム１１７は、初期条件作成プログラム１１８によりシリアル番号を作成し、ハッシュ値計算プログラム１１９により登録するデータのハッシュを計算し、暗号化プログラム１２０により登録するデータを暗号化する鍵を作成して、暗号化プログラム１２０が持っている最新の暗号化アルゴリズムにより登録するデータを暗号化し、さらにその暗号化の鍵を鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより鍵格納エリア１２８にある鍵で暗号化する。登録・更新準備プログラム１１７は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を登録実行プログラム１２３に渡す。登録実行プログラム１２３は、データベース管理プログラム１１０を使って管理テーブル１０７に、シリアル番号、暗号化された登録データを登録し、鍵テーブル１０８に、シリアル番号、登録されるデータのハッシュ値、暗号化した登録データを暗号化した鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録する。

【００２７】次に、このような構成の本システムにおいて、暗号化してデータベースに登録したデータの検索処理の概略について説明する。ユーザがクライアント１００から検索するデータを入力する。検索制御プログラム１１２が起動され、クライアント１００から入力された検索するデータが検索制御プログラム１１２に渡される。検索制御プログラム１１２が検索条件作成プログラム１１５に検索するデータを渡す。検索条件作成プログラム１１５は、ハッシュ値計算プログラム１１９により検索するデータのハッシュ値を計算し、鍵取得プログラム１２５により鍵テーブル１０８から前記ハッシュ値に一致する行の暗号化された暗号鍵と、暗号化アルゴリズム識別子を取り出す。暗号化されたデータ暗号鍵を鍵暗号鍵で復号する。復号したデータ暗号鍵と暗号化アルゴリズム識別子で検索条件を暗号化し、検索のためのＳＱＬ文を作成する。検索条件作成プログラム１１５は、作成したＳＱＬ文を検索制御プログラム１１２に渡す。検索制御プログラム１１２は、前記ＳＱＬ文を検索実行プログラム１１６に渡す。検索実行プログラム１１６は、データベース管理プログラム１１０を使って暗号化された検索条件に一致するデータを管理テーブル１０７から検索する。データベース管理プログラム１１０は、検索結果を、検索制御プログラム１１２に渡す。検索制御プログラム１１２は、検索結果を復号してクライアント１００に復号した検索結果を返す。クライアント１００は、検索結果を画面に表示する。

【００２８】次に、このような構成の本システムにおいて、暗号化してデータベースに格納したデータの更新処理の概略について説明する。ユーザがクライアント１００から更新前のデータと更新後のデータを入力する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力された更新前データと更新後のデータが登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、更新前のデータをデータ探索プログラム１１４に渡す。データ探索プラグラム１

１４は、検索条件作成プログラム１１５により更新前のデータを暗号化し、検索実行プログラム１１６により更新前のデータのシリアル番号を取り出し、登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータを登録・更新準備プログラム１１７に渡す。登録・更新準備プログラム１１７は、ハッシュ値計算プログラム１１９により、更新後のデータのハッシュ値を計算し、暗号化プログラム１２０により更新後のデータを暗号化する鍵を作成し、更新するデータを暗号化プログラム１２０が持っている最新の暗号化アルゴリズムで暗号化し、さらに鍵暗号化プログラム１２１が、その暗号化の鍵を鍵格納エリア１２８にある鍵暗号鍵で鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより暗号化する。

【００２９】登録・更新準備プログラム１１７は、更新後のデータのハッシュ値、暗号化された更新後のデータ、暗号化された更新後のデータを暗号化した鍵、更新後のデータを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータのハッシュ値、暗号化された更新後のデータ、暗号化された更新後のデータを暗号化した鍵、更新後のデータを暗号化した暗号化アルゴリズム識別子を登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を更新実行プログラム１２４に渡す。更新実行プログラム１２４は、データベース管理プログラム１１０を使って、管理テーブル１０７の暗号化された更新後のデータと鍵テーブル１０８の更新後のデータのハッシュ値、暗号化された更新後のデータを暗号化した鍵、暗号化アルゴリズム識別子をシリアル番号にしたがって更新する。

【００３０】次に、このような構成の本システムにおいて、暗号化してデータベースに格納したデータの削除処理の概略について説明する。ユーザがクライアント１００から削除するデータを入力する。削除制御プログラム１１３が起動され、クライアント１００から入力された削除するデータがこれに渡される。削除制御プログラム１１３は、削除するデータをデータ探索プログラム１１４に渡す。データ探索プログラム１１４は、検索条件作成プログラム１１５により削除するデータを暗号化し、検索実行プログラム１１６により削除するデータのシリアル番号を取り出し、削除制御プログラム１１３に渡す。削除制御プログラム１１３は、前記シリアル番号を削除条件作成プログラム１２６に渡す。削除条件作成プログラム１２６は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを削除制御プログラム１１３に渡す。削除制御プログラム１１３は、削除条件作成プログラム１２６で作成したＳＱＬ文を削除実行プログラム１２７に渡す。削除実行プログラム１２７は、データベース管理プログラム１１０を使って管理テーブル１０７と鍵テーブル１０８から渡されたシリアル番号の行を削除する。

【００３１】上述の処理をフローチャートを用いて、さらに詳細に説明する。以下の説明では、具体例として図２の管理テーブルと図３の鍵テーブルを用いた場合について説明する。図８は登録・更新プログラム１１１が実行する暗号化データベースへのデータの登録処理フローを示している。

【００３２】データ登録処理は、登録データ入力ステップ８００、登録準備ステップ８０１、登録データＳＱＬ文作成ステップ８０２およびデータベース登録ステップ８０３からなる。登録データ入力ステップ８００では、ユーザがクライアント１００から入力した登録するデータを読み込む。登録準備ステップ８０１では、シリアル番号を作成し、登録するデータのハッシュ値を計算し、登録するデータを暗号化するデータ暗号鍵を作成し、そのデータ暗号鍵で登録するデータを暗号化する。データ暗号鍵を鍵暗号鍵で暗号化する。登録データＳＱＬ文作成ステップ８０２では、登録準備ステップ８０１で作成したシリアル番号、計算したハッシュ値、暗号化されたデータ暗号鍵、暗号化された登録するデータから、管理テーブル１０７と鍵テーブル１０８に登録するＳＱＬ文を作成する。データベース登録ステップ８０３では、登録実行プログラム１２３が登録データＳＱＬ文作成ステップ８０２で作成したＳＱＬ文を実行して、データベース管理プログラム１１０により管理テーブル１０７にシリアル番号と暗号化された登録するデータを登録し、鍵テーブル１０８にシリアル番号と登録データのハッシュ値と暗号化した登録データを暗号化した鍵と暗号化アルゴリズム識別子を登録する。

【００３３】次に、登録準備ステップ８０１の処理を図９のフローチャートを使って詳細に説明する。登録準備ステップ８０１は、シリアル番号作成ステップ９００、ハッシュ値計算ステップ９０１、暗号アルゴリズム決定ステップ９０２、データ暗号化ステップ９０３および鍵暗号化ステップ９０４からなる。シリアル番号作成ステップ９００では、管理テーブル１０７と鍵テーブル１０８のそれぞれの行を関係付けるシリアル番号を作成する。ハッシュ値計算ステップ９０１では、登録するデータのハッシュ値を計算する。暗号アルゴリズム決定ステップ９０２では、暗号化プログラム１２０が今回の暗号化に使用する暗号化アルゴリズムを決定する。暗号化プログラム１２０は複数の暗号アルゴリズムを持つことができ、その中で登録・更新時の暗号化にはもっとも新しく暗号化プログラム１２０に登録された暗号アルゴリズムを使用するようにしている。データ暗号化ステップ９

０３では、登録するデータを暗号化するためのデータ暗号鍵を作成し、そのデータ暗号鍵で登録するデータを暗号化する。鍵暗号化ステップ９０４では、データ暗号化ステップ９０３で作成した鍵を鍵格納エリア１２８にある鍵暗号鍵を使って暗号化する。

【００３４】図１０は検索制御プログラム１１２が実行する暗号化データベースへのデータの検索処理フローを示している。データ検索処理は、検索データ入力ステップ１０００、ハッシュ値計算ステップ１００１、検索ＳＱＬ文作成ステップ１００２、管理テーブル検索ステップ１００３、管理テーブル一致データチェックステップ１００４、鍵テーブル検索ステップ１００５、鍵テーブル一致データチェックステップ１００６、検索結果表示ステップ１００７、シリアル番号取得ステップ１００８、全データ復号ステップ１００９からなる。検索データ入力ステップ１０００では、ユーザがクライアント１００から入力した検索するデータを読み込む。ハッシュ値計算ステップ１００１では、検索するデータのハッシュ値を計算する。検索ＳＱＬ文作成ステップ１００２では、ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行の暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を鍵テーブル１０８から取り出し（ハッシュ値についてのＳＱＬ文を作成して鍵テーブルから取り出す）、データ暗号鍵を復号し、その復号したデータ暗号鍵で検索データを暗号化して、管理テーブルを検索するＳＱＬ文を作成する。管理テーブル検索ステップ１００３では、検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文により管理テーブル１０７を検索する。管理テーブル一致データチェックステップ１００４では、検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文に一致するデータが管理テーブル１０７にあるかどうか調べる。検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文に一致するデータが管理テーブル１０７にある場合、シリアル番号取得ステップ１００８に進む。シリアル番号取得ステップ１００８では、管理テーブル１０７で一致したデータの鍵テーブル１０８のシリアル番号を取り出す。全データ復号ステップ１００９では、シリアル番号取得ステップ１００８で取り出したシリアル番号からすべての暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出し、鍵暗号鍵で復号したデータ暗号鍵と、暗号化アルゴリズムにより管理テーブルの暗号化されたデータをすべて復号化する。管理テーブル検索ステップ１００３に戻り処理を続ける。

【００３５】検索ＳＱＬ文作成ステップ１００２で作成したＳＱＬ文に一致するデータが管理テーブル１０７にない場合、鍵テーブル検索ステップ１００５に進み、鍵テーブル１０８を検索し、ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行がまだあるか調べる。鍵テーブル一致データチェックステップ１００６では、鍵テーブル検索ステップ１００５の検索結果を判定する。ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行がある場合、検索ＳＱＬ文作成ステップ１００２に戻り、新たなデータ暗号鍵を使って検索処理を行う。ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行がない場合、検索結果表示ステップ１００７に進む。検索結果表示ステップ１００７では、クライアントの画面に検索結果が表示される。

【００３６】次に、検索ＳＱＬ文作成ステップ１００２の処理を図１１のフローチャートを使って詳細に説明する。検索ＳＱＬ文作成ステップ１００２は、暗号化情報取得ステップ１１００および暗号化検索データ作成ステップ１１０１からなる。暗号化情報取得ステップ１１００では、鍵テーブル１０８を検索して、ハッシュ値計算ステップ１００１で計算したハッシュ値に一致する行の暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出し、暗号化されたデータ暗号鍵を鍵暗号鍵で復号する。暗号化検索データ作成ステップ１１０１では、復号したデータ暗号鍵と、暗号化アルゴリズムにより検索条件を暗号化する。

【００３７】暗号化されているデータベースを検索する方法として、暗号化された管理テーブルからデータを一つずつ取り出し、それを復号しながら検索条件に一致するかどうかを調べる方法と検索条件をあらかじめ暗号鍵で暗号化しておき、その暗号化した検索条件で暗号化された管理テーブルを検索する方法がある。前者の方法では、管理テーブルからのデータの取り出しごとに復号の処理が発生するため、データベースの検索性能を大きく悪化させる。後者の方法では、検索条件を暗号化する処理が一回発生する以外は、暗号化されていないデータベースとほぼおなじ検索性能を出すことができる。このため、暗号化された管理テーブルの検索の実現には、後者の方法が性能的に優れている。本実施例においては、後者の方式について説明した。

【００３８】本発明の方式のデータ構造では特定のデータ集合ごとに暗号化に使用する鍵が異なるため、鍵テーブル１０８から検索条件を暗号化する鍵を取り出す手段としてデータのハッシュ値を利用して鍵テーブル１０８からデータ暗号鍵を検索するようにした。

【００３９】図１２は登録・更新制御プログラム１１１が実行する暗号化データベースへのデータの更新処理フローを示している。データ更新処理は、更新データ入力ステップ１２００、更新前データ探索ステップ１２０１、一致データチェックステップ１２０２、シリアル番号取得ステップ１２０３、更新後データ暗号化ステップ１２０４、更新ＳＱＬ文作成ステップ１２０５およびデータベース登録ステップ１２０６からなる。更新データ入力ステップ１２００では、ユーザがクライアント１００から入力した更新前のデータと更新後のデータを読み込む。更新前データ探索ステップ１２０１では、更新前のデータを管理テーブル１０７から検索する。一致デー

タチェックステップ１２０２では、更新前データ探索ステップ１２０１で検索した結果を判定する。更新前データ探索ステップ１２０１で検索した更新前データが管理テーブル１０７にない場合、更新処理を終了する。

【００４０】更新前データ探索ステップ１２０１で検索した更新前データが管理テーブル１０７にある場合、シリアル番号取得ステップ１２０３に進む。シリアル番号取得ステップでは、更新前データ探索ステップ１２０１で検索した更新前データのシリアル番号を取得する。更新後データ暗号化ステップ１２０４では、更新後のデータのハッシュ値を計算した後、更新後のデータをデータ暗号鍵で暗号化する。データ暗号鍵を鍵暗号鍵で暗号化する。更新ＳＱＬ文作成ステップ１２０５では、シリアル番号取得ステップ１２０３で取得したシリアル番号と更新後データ暗号化ステップ１２０４で作成した暗号化した更新後のデータを使って、更新するデータのＳＱＬ文を作成する。データベース登録ステップ１２０６では、データベース管理プログラム１１０により管理テーブル１０７のデータを更新実行プログラム１２４が更新データＳＱＬ文作成ステップ１２０５で作成したＳＱＬ文を実行して更新し、鍵テーブル１０８の更新後のデータのハッシュ値と暗号化したデータ暗号鍵と、暗号化アルゴリズム識別子を更新する。

【００４１】次に、更新前データ探索ステップ１２０１の処理を図１３のフローチャートを使って詳細に説明する。更新前データ探索ステップ１２０１は、ハッシュ値計算ステップ１３００、暗号化検索条件作成ステップ１３０１、管理テーブル検索ステップ１３０２、および一致データチェックステップ１３０３からなる。ハッシュ値計算ステップ１３００では、検索条件作成プログラム１１５を起動し、更新前データのハッシュ値を計算する。暗号化検索条件作成ステップ１３０１では、検索条件作成プログラム１１５を起動して、鍵テーブル１０８を検索してハッシュ値に一致する暗号化されたデータ暗号鍵と、暗号化アルゴリズム識別子を取り出す。鍵暗号鍵でデータ暗号鍵を復号し、復号したデータ暗号鍵と、暗号化アルゴリズム１１６で検索条件を暗号化する。管理テーブル検索ステップ１３０２では、検索実行プログラムを起動し、暗号化検索条件作成ステップ１３０１で暗号化したＳＱＬ文で管理テーブル１０７を検索する。一致データチェックステップ１３０３では、管理テーブル１０７に暗号化検索条件作成ステップ１３０１で作成したＳＱＬ文の検索条件に一致するデータがあるかどうかを調べる。暗号化検索条件作成ステップ１３０１で作成したＳＱＬ文の検索条件に一致するデータがある場合は、終了する。

【００４２】暗号化検索条件作成ステップ１３０１で作成したＳＱＬ文の検索条件に一致するデータがない場合は、ハッシュ値に一致する別の暗号化されたデータ暗号鍵と暗号化アルゴリズム識別子を取り出す。暗号化されたデータ暗号鍵を鍵暗号鍵で復号し、復号したデータ暗号鍵と、前記暗号化アルゴリズム識別子に対応する暗号化アルゴリズムで検索条件を暗号化し、その暗号化した検索条件で再度管理テーブル１０７を検索する。

【００４３】次に、更新後データ暗号化ステップ１２０４の処理を図１４のフローチャートを使って詳細に説明する。更新後データ暗号化ステップ１２０４は、ハッシュ値計算ステップ１４００、暗号アルゴリズム決定ステップ１４０１、データ暗号化ステップ１４０２および鍵暗号化ステップ１４０３からなる。ハッシュ値計算ステップ１４００では、更新後のデータのハッシュ値を計算する。暗号アルゴリズム決定ステップ１４０１では、暗号化プログラム１２０が今回の暗号化に使用する暗号化アルゴリズムを決定する。暗号化プログラム１２０は複数の暗号アルゴリズムを持つことができ、その中で登録・更新時の暗号化にはもっとも新しく暗号化プログラム１２０に登録された暗号アルゴリズムを使用するようにしている。データ暗号ステップ１４０２では、データ暗号鍵を作成し、管理テーブル１０７に登録するデータを暗号化する。鍵暗号化ステップ１４０３では、データ暗号鍵を鍵格納エリア１２８にある鍵暗号鍵により暗号化する。

【００４４】図１５は、削除制御プログラム１１３が実行する暗号化データベースのデータの削除処理フローを示している。データ削除処理は、削除データ入力ステップ１５００、削除データ探索ステップ１５０１、一致データチェックステップ１５０２、シリアル番号取得ステップ１５０３、削除ＳＱＬ文作成ステップ１５０４およびデータベース削除実行ステップ１５０５からなる。削除データ入力ステップ１５００では、ユーザがクライアント１００から入力した削除するデータを読み込む。削除データ探索ステップ１５０１では、削除データを検索する。一致データチェックステップ１５０２では、削除データ探索ステップ１５０１で検索した削除データが管理テーブル１０７にあるかどうかチェックする。削除データ探索ステップ１５０１で検索した削除データが管理テーブル１０７にない場合、削除処理を終了する。

【００４５】削除データ探索ステップ１５０１で検索した削除データが管理テーブル１０７にある場合、シリアル番号取得ステップ１５０３に進む。シリアル番号取得ステップ１５０３では、削除データ探索ステップ１５０１で検索した削除データのシリアル番号を取得する。削除ＳＱＬ文作成ステップ１５０４では、シリアル番号取得ステップ１５０３で取得したシリアル番号を使って削除ＳＱＬ文を作成する。データベース削除実行ステップ１５０５では、削除ＳＱＬ文作成ステップ１５０４で作成した削除ＳＱＬ文を使って管理テーブル１０７と鍵テーブル１０８からシリアル番号取得ステップ１５０３で取得したシリアル番号の行を削除する。削除データ探索ステップ１５０１に戻り、処理を続ける。

【００４６】以上、本実施例の特徴として、管理テーブルとそのテーブルの特定の値の集合（フィールド、行、列など）に関する暗号化のための情報（暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値）をもつ鍵テーブルにより秘密情報を管理することを特徴とするデータベース構造、およびその構成におけるデータの登録処理、検索処理、更新処理、削除処理について説明した。本実施例によれば、前記データベース構造を用いて、データ登録または更新時に暗号鍵を動的に変更し、暗号化のための情報を管理テーブルと別管理することにより、暗号化されたデータベースの安全性を高めることができる。また、管理テーブルの特定の値の集合ごとに異なる暗号化アルゴリズムを使用することが可能となり、さらにデータベース稼動中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことも可能である。よって本実施例を適用することにより、十分なデータベースの安全性を確保することができる。

【００４７】次に、本発明の第二の実施例について説明する。本実施例は図１に示した第一の実施例と同様の構成をとるが、検索時にもデータ暗号鍵を更新するようにした部分が第一の実施例と異なる。第二の実施例の検索方式について図１６を使って説明する。第二の実施例のデータ検索処理は、検索データ入力ステップ１６００、ハッシュ値計算ステップ１６０１、検索ＳＱＬ文作成ステップ１６０２、管理テーブル検索ステップ１６０３、管理テーブル一致データチェックステップ１６０４、鍵テーブル検索ステップ１６０５、鍵テーブル一致データチェックステップ１６０６、検索結果表示ステップ１６０７、シリアル番号取得ステップ１６０８、全データ復号ステップ１６０９、鍵テーブル登録ステップ１６１０および管理テーブル登録ステップ１６１１からなる。

【００４８】図１６の検索データ入力ステップ１６００から全データ復号ステップ１６０９までの処理は、図１０の検索データ入力ステップ１０００から全データ復号ステップ１００９までの処理にそれぞれ対応し、同じ処理を行う。鍵テーブル登録ステップ１６１０において、検索条件に一致したデータを暗号化するためのデータ暗号鍵を新たに作成し、そのデータ暗号鍵を鍵暗号鍵で暗号化して、シリアル番号、暗号化アルゴリズム識別子とともに鍵テーブル１０８に登録する。管理テーブル登録ステップ１６１１において、鍵テーブル登録ステップ１６１０で作成したデータ暗号鍵を使って検索条件に一致したデータを暗号化して管理テーブル１０７に登録したあと、管理テーブル検索ステップ１６０３に戻って管理テーブル１０７の検索を続ける。

【００４９】以上、第二の実施例として、データ登録または更新時だけではなく検索時にも暗号鍵を変更する方式について説明した。本実施例によれば、前記データベース構造を用いて、データ登録、更新または検索時に暗号鍵を動的に変更することにより、第一の実施例のデータ登録または更新のときよりも頻繁に暗号鍵を更新するため暗号化されたデータベースの安全性をさらに高めることができる。

【００５０】次に、本発明の第三の実施例について説明する。第一の実施例では、新しい暗号化アルゴリズムが追加された場合に直ちにそれを使用していた。本実施例は図１に示した第一の実施例と同様の構成をとるが、暗号化アルゴリズムを上位で指定し、指定された暗号化アルゴリズムで暗号化するようにした部分が第一の実施例と異なる。

【００５１】図１を使って本実施例について説明する。データベースに暗号化して格納するデータの登録処理の概略について説明する。ユーザがクライアント１００からデータベースに登録するデータを入力し、暗号化アルゴリズム識別子を指定する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力された登録するデータと指定された暗号化アルゴリズム識別子が登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、登録・更新準備プログラム１１７に登録するデータと暗号化アルゴリズム識別子を渡す。登録・更新準備プログラム１１７は、初期条件作成プログラム１１８によりシリアル番号を作成し、ハッシュ値計算プログラム１１９により登録するデータのハッシュを計算し、暗号化プログラム１２０によりクライアント１００で指定された暗号化アルゴリズム識別子に基づくデータ暗号鍵を作成して、この鍵を使用して登録するデータを暗号化し、さらにそのデータ暗号鍵を鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより鍵格納エリア１２８にある鍵暗号鍵で暗号化する。

【００５２】登録・更新準備プログラム１１７は、シリアル番号、登録されるデータのハッシュ値、暗号化された登録データ、データ暗号鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、これらのデータを登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を登録実行プログラム１２３に渡す。登録実行プログラム１２３は、データベース管理プログラム１１０を使って管理テーブル１０７に、シリアル番号、暗号化された登録データを登録し、鍵テーブル１０８に、シリアル番号、登録されるデータのハッシュ値、データ暗号鍵、登録データを暗号化した暗号化アルゴリズム識別子を登録する。

【００５３】次に、第三の実施例における、データの更新処理の概略について説明する。ユーザがクライアント

１００から更新前のデータ、更新後のデータ、および更新後のデータの暗号アルゴリズム識別子を指定する。登録・更新制御プログラム１１１が起動され、クライアント１００から入力されたパラメータが登録・更新制御プログラム１１１に渡される。登録・更新制御プログラム１１１は、更新前のデータをデータ探索プログラム１１４に渡す。データ探索プラグラム１１４は、検索条件作成プログラム１１５により更新前のデータを暗号化し、検索実行プログラムにより更新前のデータのシリアル番号を取り出し、登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータ、更新後のデータを暗号化する暗号化アルゴリズム識別子を登録・更新準備プログラム１１７に渡す。

【００５４】登録・更新準備プログラム１１７は、ハッシュ値計算プログラムにより、更新後のデータのハッシュ値を計算し、暗号化プログラム１２０によりクライアント１００で指定された更新後のデータを暗号化する暗号化アルゴリズムに基づくデータ暗号鍵を作成して、更新するデータを暗号化し、さらに鍵暗号化プログラム１２１が、そのデータ暗号鍵を鍵格納エリア１２８にある鍵で鍵暗号化プログラム１２１が持っている暗号化アルゴリズムにより暗号化する。登録・更新準備プログラム１１７は、更新後のデータのハッシュ値、暗号化されたデータ、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、シリアル番号、更新後のデータのハッシュ値、暗号化されたデータ、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を登録・更新条件作成プログラム１２２に渡す。登録・更新条件作成プログラム１２２は、渡されたデータから管理テーブル１０７と鍵テーブル１０８のためのＳＱＬ文をそれぞれ作成し、それを登録・更新制御プログラム１１１に渡す。登録・更新制御プログラム１１１は、登録・更新条件作成プログラム１２２で作成したＳＱＬ文を更新実行プログラム１２４に渡す。更新実行プログラム１２４は、データベース管理プログラム１１０を使って、管理テーブル１０７のデータと鍵テーブル１０８のデータのハッシュ値、暗号化されたデータ暗号鍵、暗号化アルゴリズム識別子を更新する。

【００５５】以上で説明したように、第三の実施例によれば、上位アプリケーションが、自由に暗号化アルゴリズムを指定することができ、柔軟に暗号化アルゴリズムを選択することができる。

【００５６】以上、本発明の特徴として、管理テーブルとそのテーブルの特定のデータ集合（フィールド、行、列など）に関する暗号化のための情報（暗号鍵、暗号化アルゴリズム識別子、データのハッシュ値）をもつ鍵テーブルにより秘密情報を管理することを特徴とするデータベース構造、その構成における暗号化されたデータの登録、検索、更新、削除、暗号鍵の動的な更新方法、およびデータベース稼動中の暗号化アルゴリズムの切り替え方法について説明した。本発明が用いるデータベース管理システムとしては、リレーショナルデータベースおよびオブジェクト指向データベースのいずれでも実施可能である。

【００５７】オブジェクト指向データベースを利用する場合には、鍵テーブル１０８の定義にオブジェクトを利用することになる。また、鍵テーブル１０８に、ハッシュアルゴリズムのフィールドを追加して、ハッシュアルゴリズムを暗号化アルゴリズムとともに特定のデータ集合ごとに変更することもできる。

【００５８】本発明によれば、前記データベース構造を用いて、暗号鍵を動的に変更し、暗号化のための情報を管理テーブルと別管理することにより、暗号化されたデータベースの安全性を高めることができる。また、特定のデータ集合ごとに新しい暗号化アルゴリズムに変更することが可能となり、データベース稼動中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことも可能である。よって本発明を適用することにより、十分なデータベースの安全性を確保することができる。さらに将来より強固な暗号化アルゴリズムが発明された場合にも、管理データ暗号用のアルゴリズムを動的により強固な方式に切り替えていくことができる。

【００５９】

【発明の効果】本発明によれば、暗号化されたデータベースにおいて、データベース稼働中に暗号鍵および暗号化アルゴリズムの切り替えを動的に行うことができ、柔軟性を持つ安全な秘密情報管理データベースを作成することができる。

【図面の簡単な説明】

【図１】本発明のデータベースの秘密情報管理方式の実施の一形態の構成を示す図である。

【図２】フィールドごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図３】フィールドごとに暗号化したデータベースの鍵テーブルを説明するための図である。

【図４】行ごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図５】行ごとに暗号化したデータベースの鍵テーブルを説明するための図である。

【図６】列ごとに暗号化したデータベースの管理テーブルを説明するための図である。

【図７】列ごとに暗号化したデータベースの鍵テーブルを説明するための図である。

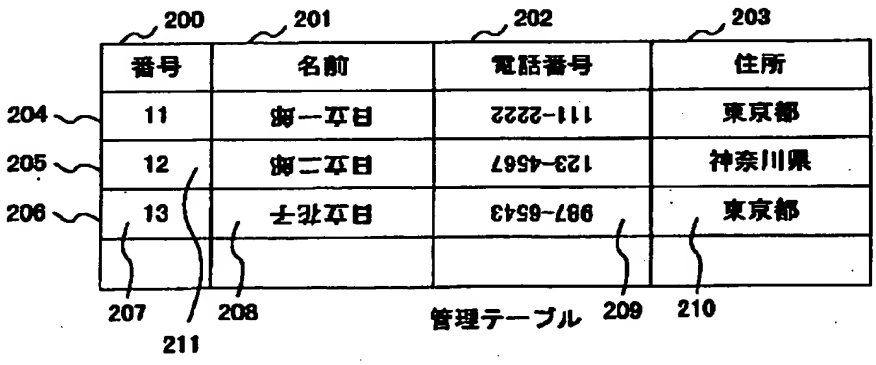
【図８】本発明により行われるデータベースのデータ登録の手順を説明するフローチャートである。

【図９】本発明により行われるデータベースのデータ登録時の登録・更新準備プログラムの手順を説明するフローチャートである。

【図１０】本発明により行われるデータベースのデータ検索の手順を説明するフローチャートである。
【図１１】本発明により行われるデータベースのデータ検索時の検索条件作成プログラムの手順を説明するフローチャートである。
【図１２】本発明により行われるデータベースのデータ更新の手順を説明するフローチャートである。
【図１３】本発明により行われるデータベースのデータ更新時のデータ探索プログラムの手順を説明するフローチャートである。
【図１４】本発明により行われるデータベースのデータ更新時の登録・更新準備プログラムの手順を説明するフローチャートである。
【図１５】本発明により行われるデータベースのデータ削除の手順を説明するフローチャートである。
【図１６】本発明により行われるデータベースの暗号鍵と暗号化アルゴリズムの変更を伴うデータ検索の手順を説明するフローチャートである。
【符号の説明】
１００　クライアント
１０１　ＬＡＮ
１０２　ＬＡＮアダプタ
１０３　サーバ
１０４　ＣＰＵ
１０５　バス
１０６　磁気ディスク装置
１０７　管理テーブル
１０８　鍵テーブル
１０９　主メモリ
１１０　データベース管理プログラム
１１１　登録・更新制御プログラム
１１２　検索制御プログラム
１１３　削除制御プログラム
１１４　データ探索プログラム
１１５　検索条件作成プログラム
１１６　検索実行プログラム
１１７　登録・更新準備プログラム
１１８　初期条件作成プログラム
１１９　ハッシュ値計算プログラム
１２０　暗号化プログラム
１２１　鍵暗号化プログラム
１２２　登録・更新条件作成プログラム
１２３　登録実行プログラム
１２４　更新実行プログラム
１２５　鍵取得プログラム
１２６　削除条件作成プログラム
１２７　削除実行プログラム
１２８　鍵格納エリア

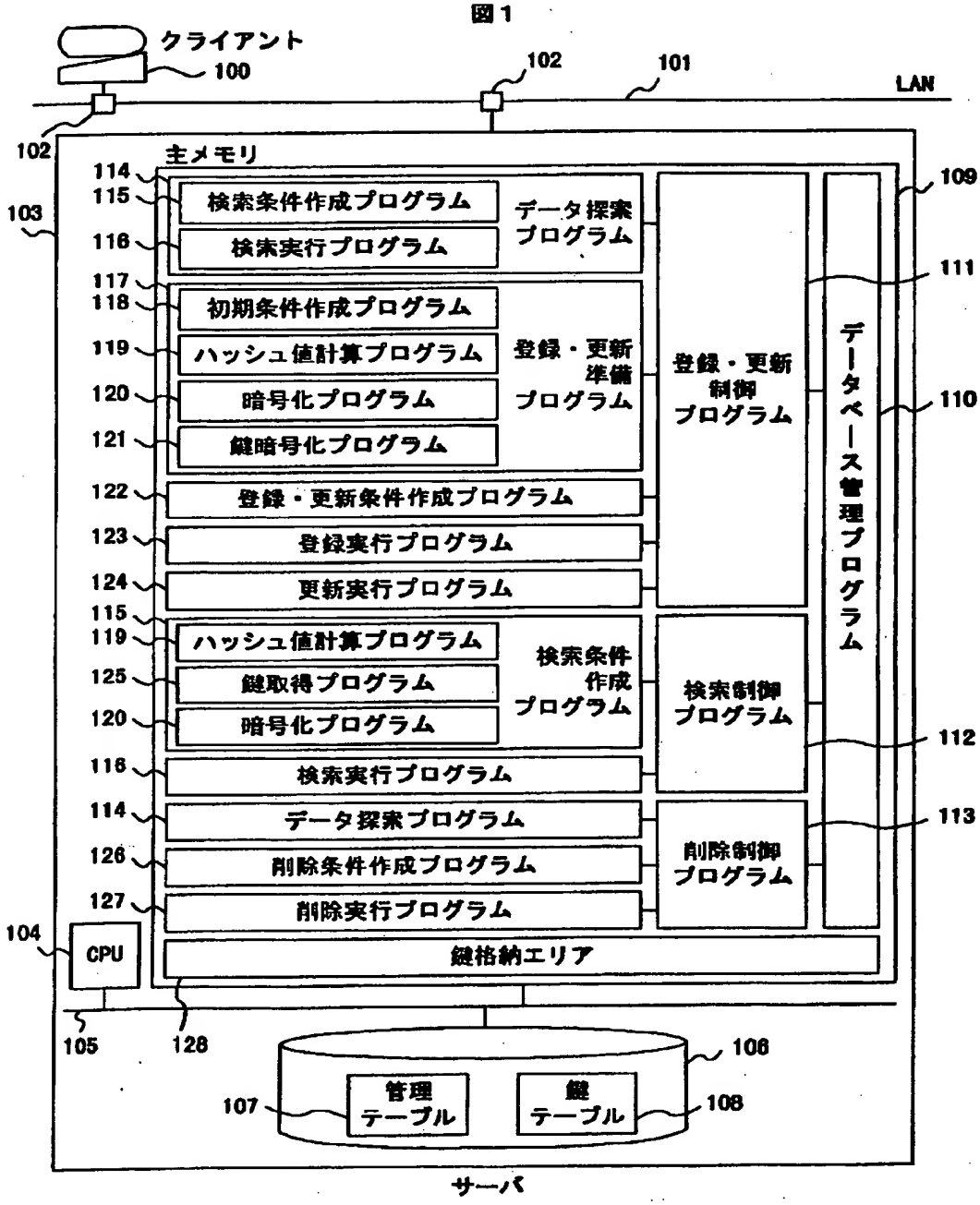
【図２】

図２



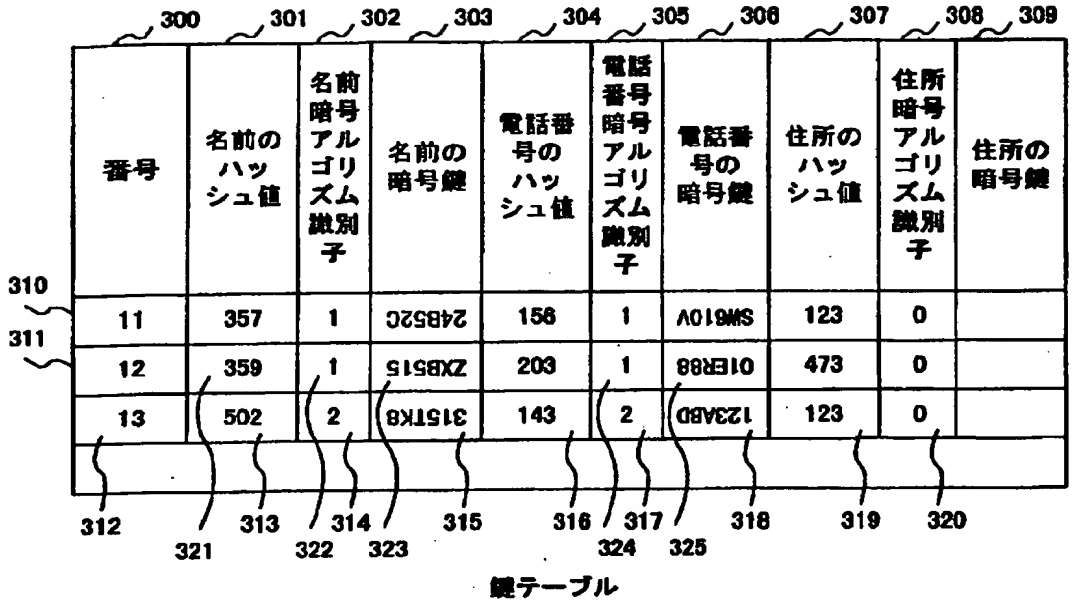
【図1】

図1


クライアント
100
102
101
LAN
102
主メモリ
103
114
115
検索条件作成プログラム
データ探索プログラム
116
検索実行プログラム
117
118
初期条件作成プログラム
119
ハッシュ値計算プログラム
登録・更新準備プログラム
120
暗号化プログラム
121
鍵暗号化プログラム
122
登録・更新条件作成プログラム
123
登録実行プログラム
124
更新実行プログラム
登録・更新制御プログラム
109
111
データベース管理プログラム
110
115
119
ハッシュ値計算プログラム
125
鍵取得プログラム
検索条件作成プログラム
120
暗号化プログラム
検索制御プログラム
112
116
検索実行プログラム
114
データ探索プログラム
113
126
削除条件作成プログラム
削除制御プログラム
127
削除実行プログラム
104
CPU
鍵格納エリア
105
128
106
107
管理テーブル
鍵テーブル
108
サーバ

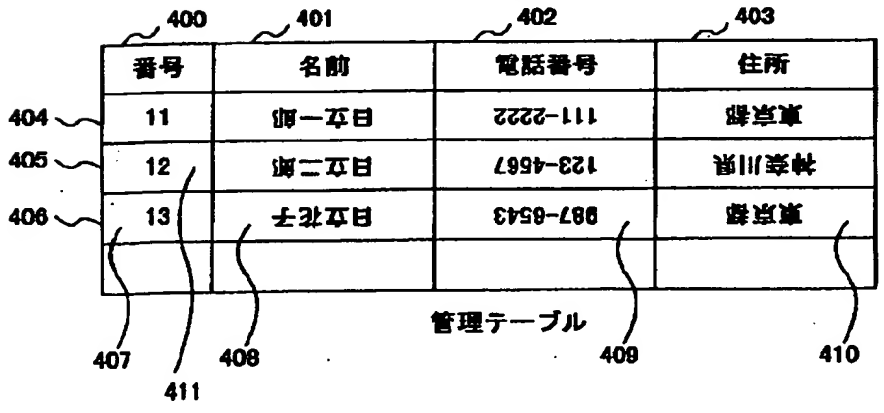
【図3】

図3


300
301
302
303
304
305
306
307
308
309
番号
名前のハッシュ値
名前暗号アルゴリズム識別子
名前の暗号鍵
電話番号のハッシュ値
電話番号暗号アルゴリズム識別子
電話番号の暗号鍵
住所のハッシュ値
住所暗号アルゴリズム識別子
住所の暗号鍵
310
311
11
357
1
24852C
156
1
SM61OV
123
0
12
359
1
ZXB515
203
1
OIER88
473
0
13
502
2
315TK8
143
2
123ABD
123
0
312
321
313
322
314
323
315
316
324
317
325
318
319
320
鍵テーブル

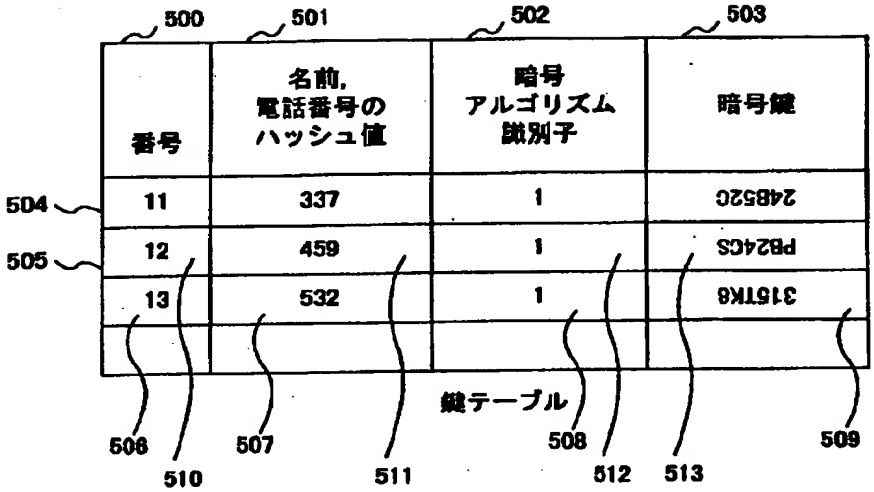
【図4】

図4


400
401
402
403
番号
名前
電話番号
住所
404
11
日立一郎
111-2222
東京都
405
12
日立二郎
123-4567
神奈川県
406
13
日立花子
987-6543
東京都
407
411
408
409
410
管理テーブル

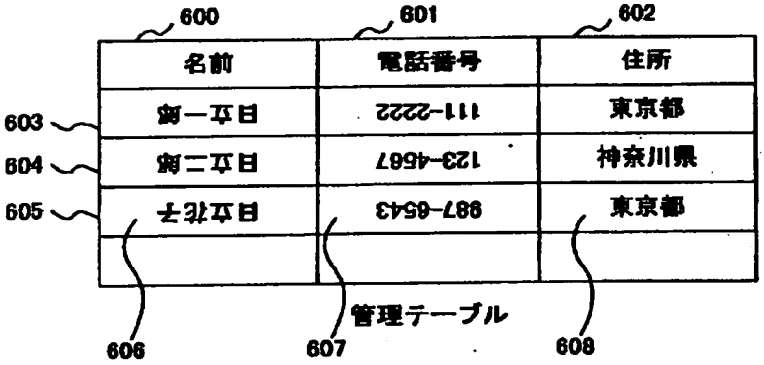
【図5】

図5



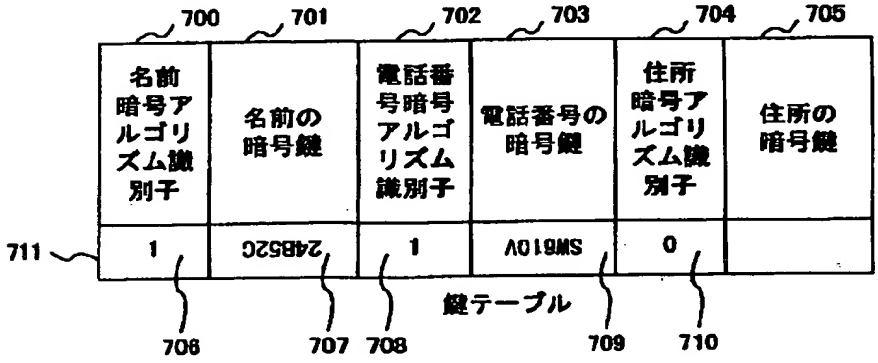
【図6】

図6



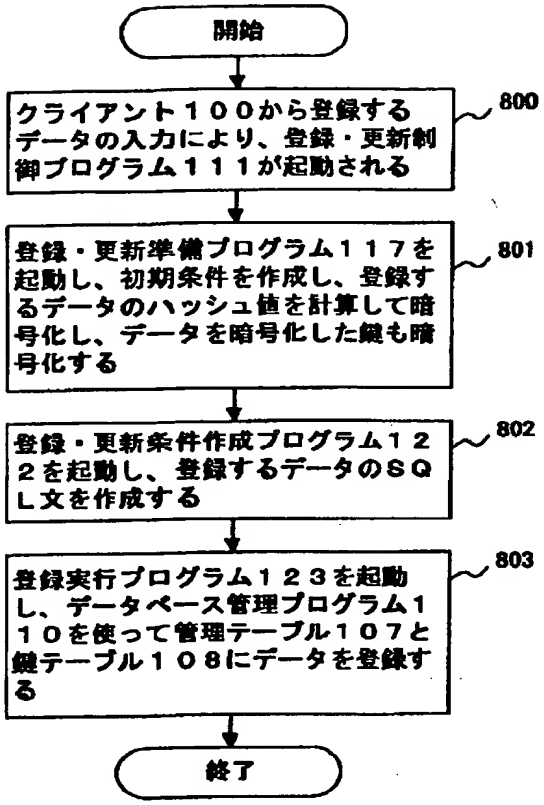
【図7】

図7



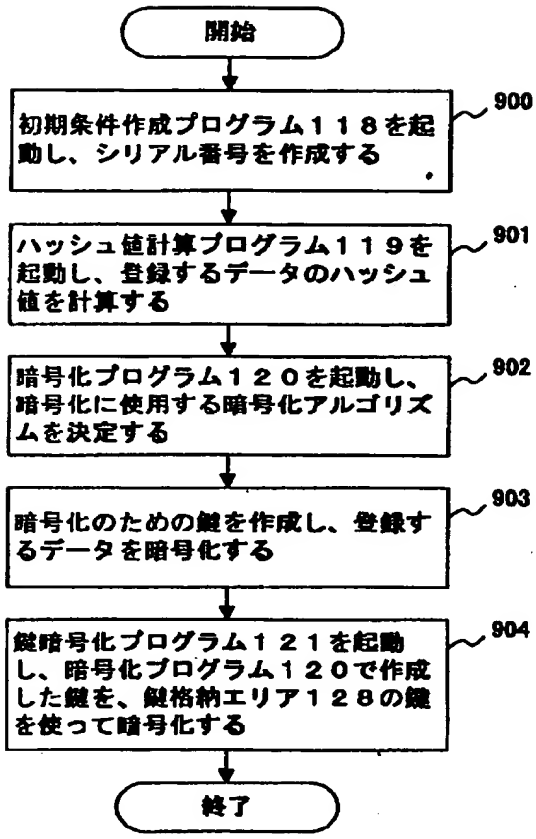
【図8】

図8



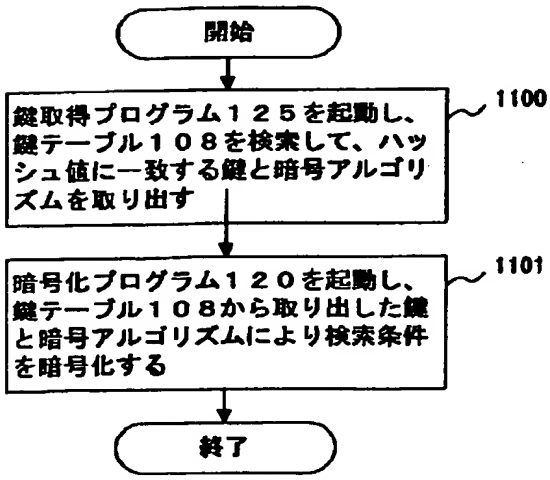
【図9】

図9



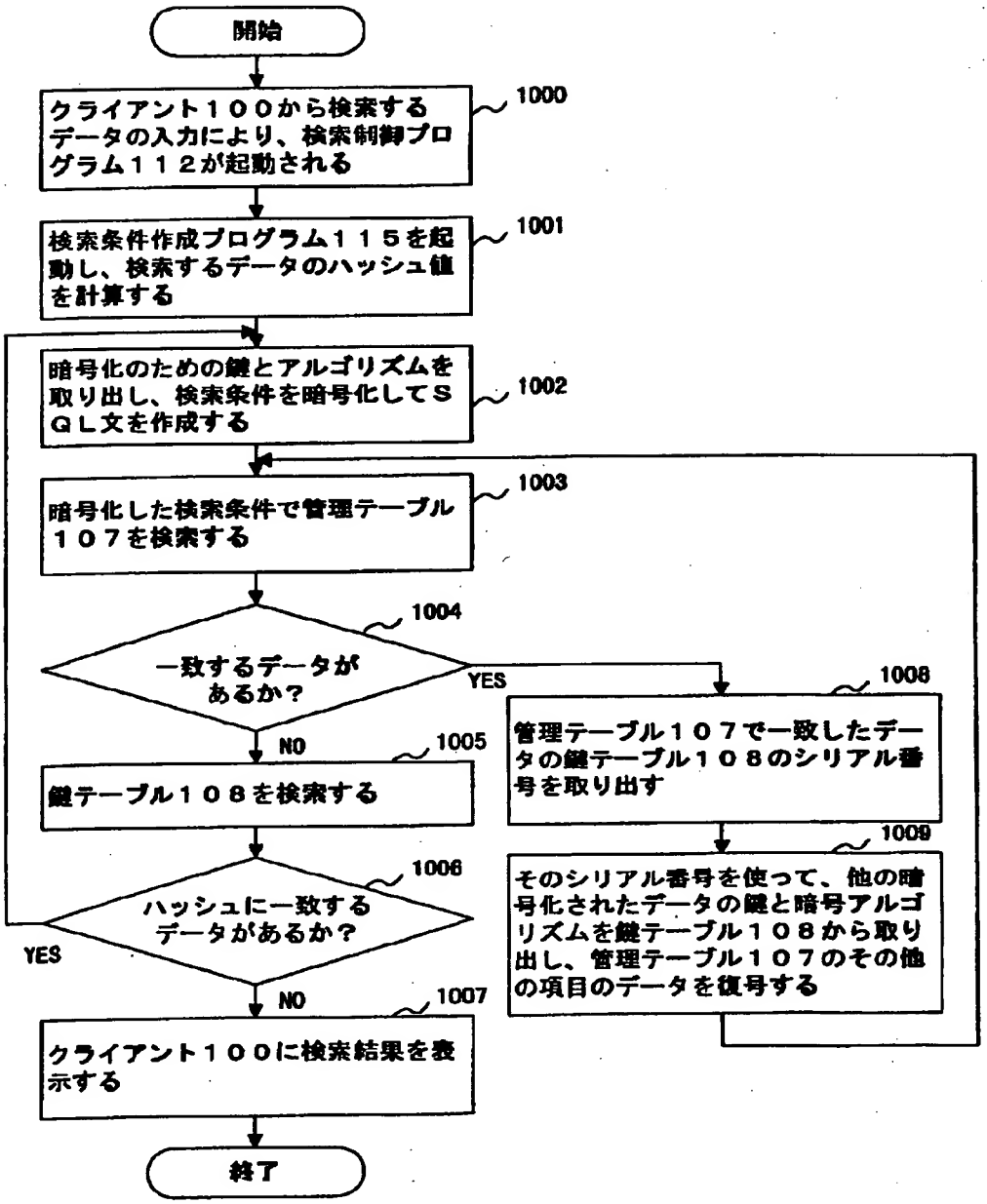
【図11】

図11



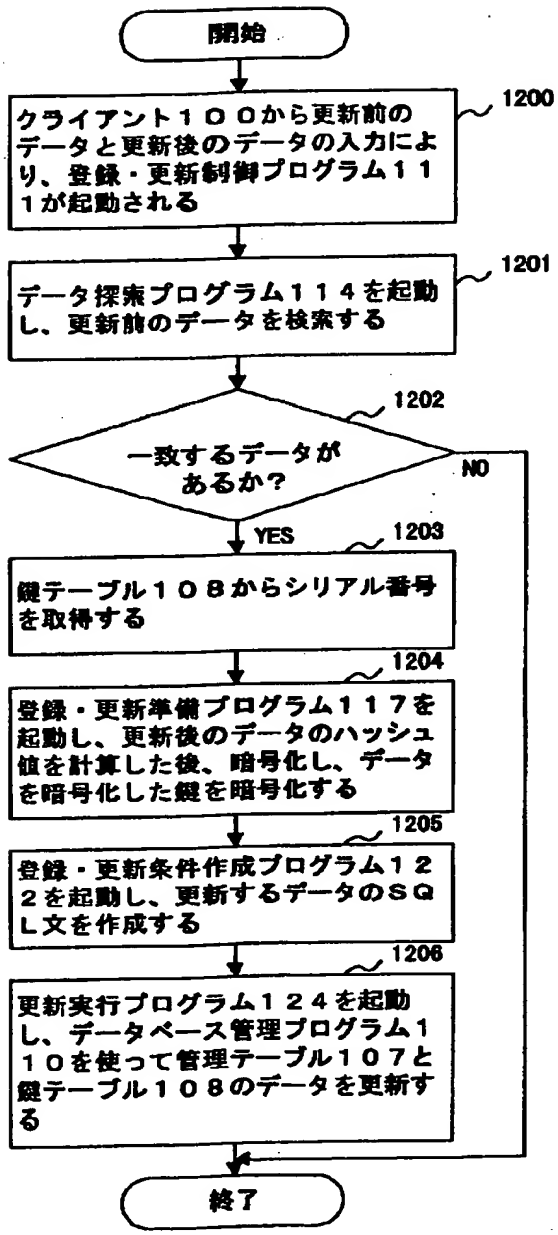
【図10】

図10


開始
クライアント１００から検索するデータの入力により、検索制御プログラム１１２が起動される
1000
検索条件作成プログラム１１５を起動し、検索するデータのハッシュ値を計算する
1001
暗号化のための鍵とアルゴリズムを取り出し、検索条件を暗号化してＳＱＬ文を作成する
1002
暗号化した検索条件で管理テーブル１０７を検索する
1003
一致するデータがあるか？
1004
YES
NO
管理テーブル１０７で一致したデータの鍵テーブル１０８のシリアル番号を取り出す
1008
鍵テーブル１０８を検索する
1005
そのシリアル番号を使って、他の暗号化されたデータの鍵と暗号アルゴリズムを鍵テーブル１０８から取り出し、管理テーブル１０７のその他の項目のデータを復号する
1009
ハッシュに一致するデータがあるか？
1006
YES
NO
クライアント１００に検索結果を表示する
1007
終了

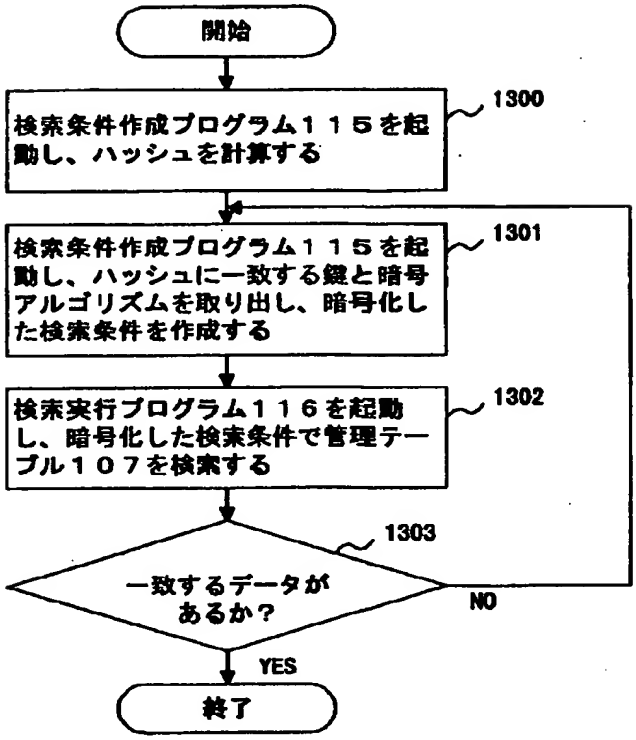
【図12】

図12



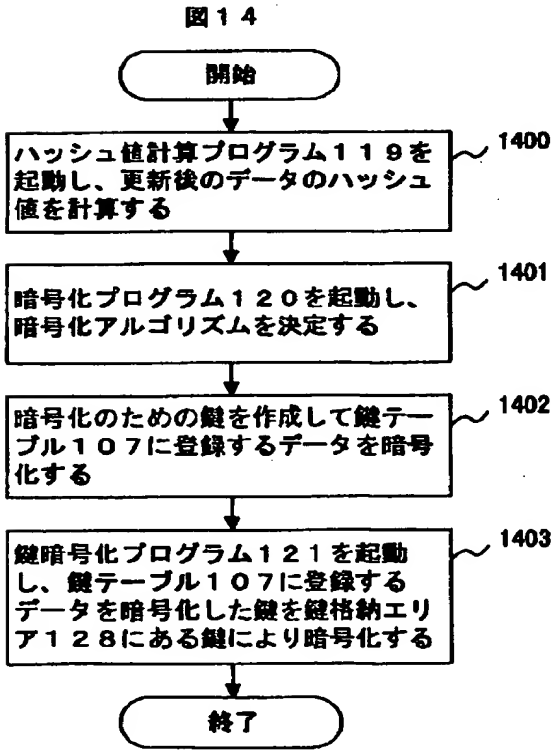
【図13】

図13



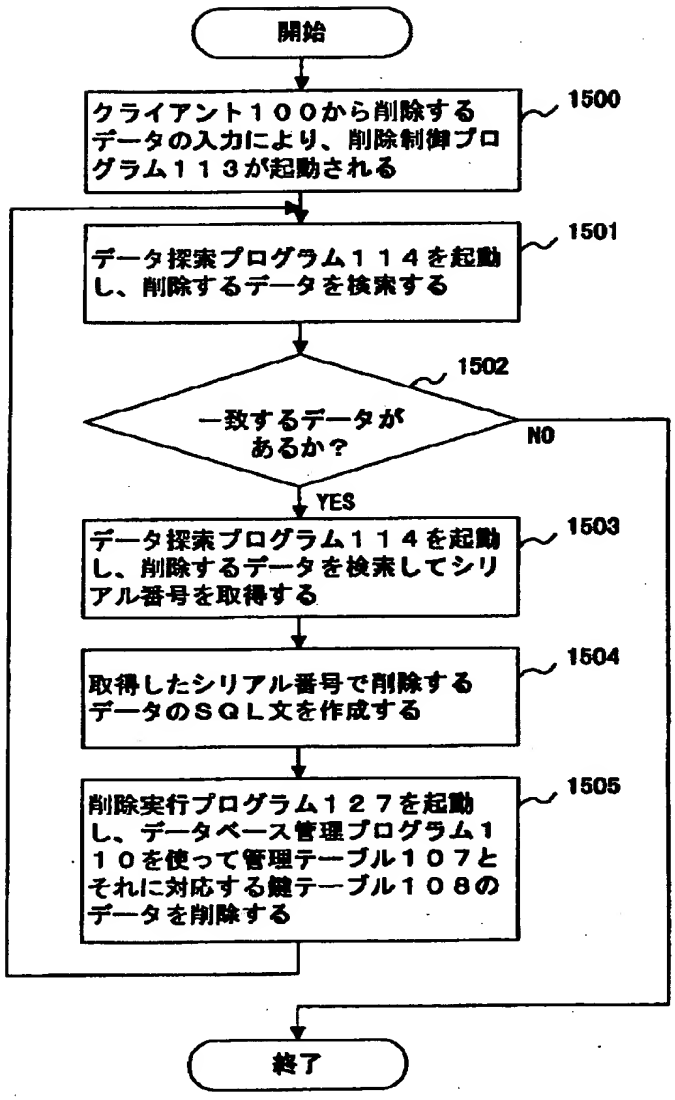
【図14】

図14



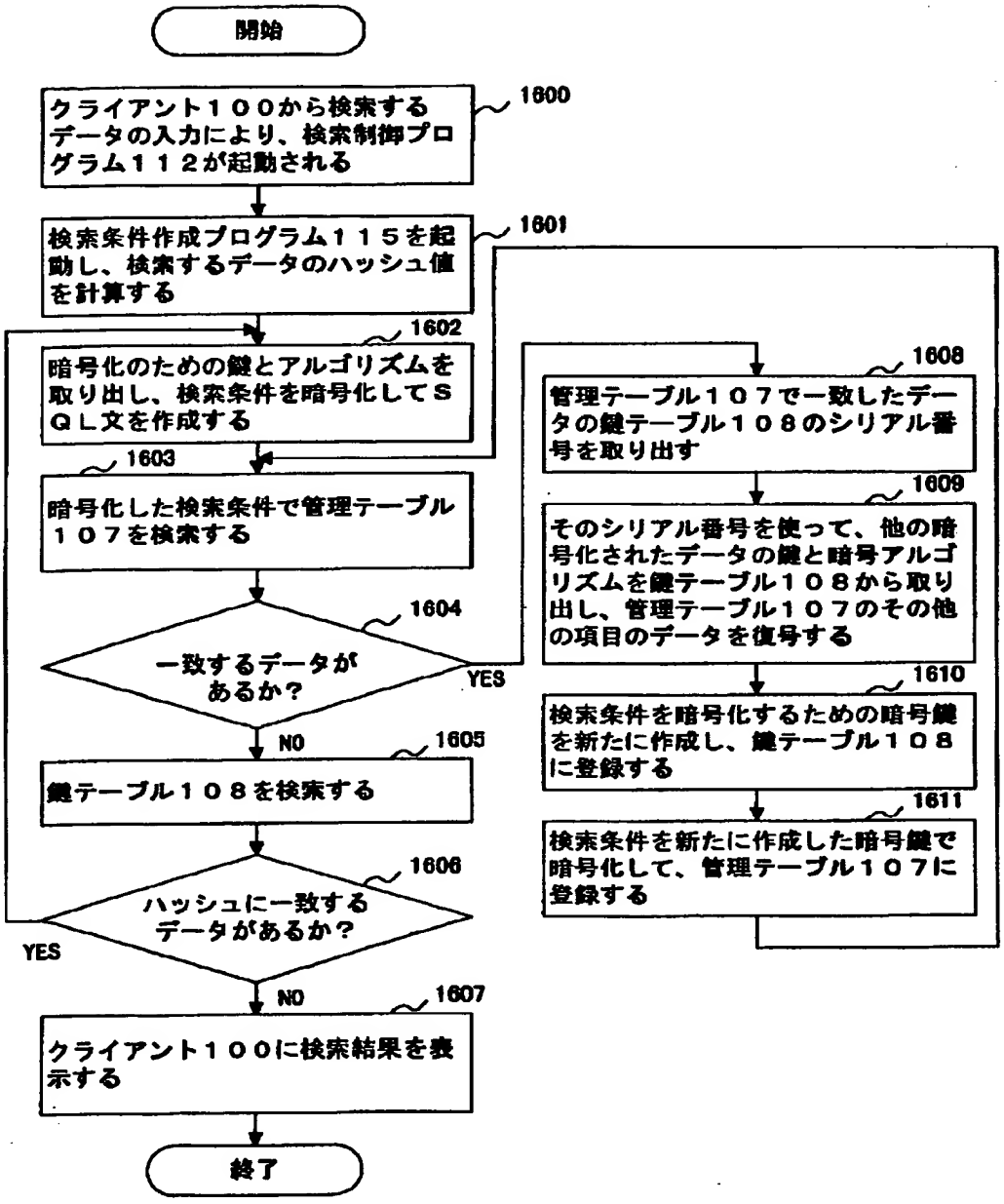
【図15】

図15


開始
クライアント100から削除するデータの入力により、削除制御プログラム113が起動される
1500
データ探索プログラム114を起動し、削除するデータを検索する
1501
一致するデータがあるか？
1502
NO
YES
データ探索プログラム114を起動し、削除するデータを検索してシリアル番号を取得する
1503
取得したシリアル番号で削除するデータのSQL文を作成する
1504
削除実行プログラム127を起動し、データベース管理プログラム110を使って管理テーブル107とそれに対応する鍵テーブル108のデータを削除する
1505
終了

【図16】

図16


開始
クライアント100から検索するデータの入力により、検索制御プログラム112が起動される
1600
検索条件作成プログラム115を起動し、検索するデータのハッシュ値を計算する
1601
暗号化のための鍵とアルゴリズムを取り出し、検索条件を暗号化してSQL文を作成する
1602
暗号化した検索条件で管理テーブル107を検索する
1603
一致するデータがあるか？
1604
YES
NO
鍵テーブル108を検索する
1605
ハッシュに一致するデータがあるか？
1606
YES
NO
クライアント100に検索結果を表示する
1607
終了
管理テーブル107で一致したデータの鍵テーブル108のシリアル番号を取り出す
1608
そのシリアル番号を使って、他の暗号化されたデータの鍵と暗号アルゴリズムを鍵テーブル108から取り出し、管理テーブル107のその他の項目のデータを復号する
1609
検索条件を暗号化するための暗号鍵を新たに作成し、鍵テーブル108に登録する
1610
検索条件を新たに作成した暗号鍵で暗号化して、管理テーブル107に登録する
1611